The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
8/11/2009

SUBJECT:
Multiple Vulnerabilities in Windows Internet Name Service (WINS) Could Allow Remote Code Execution (MS09-039)

OVERVIEW:
Multiple vulnerabilities have been discovered in the Windows Internet Name Service (WINS). WINS is an essential core service that translates computer names to numeric addresses which are needed for computers to communicate with each other. Successful exploitation of these vulnerabilities could allow an attacker to take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts. Failed exploitation attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:
Windows 2000 Server
Windows Server 2003

RISK:

Government:
Large and medium government entities: High
Small government entities: High

Businesses:
Large and medium business entities: High
Small business entities: High

Home users: N/A

DESCRIPTION:
Two vulnerabilities have been discovered in the Windows Internet Name Service (WINS). Successful exploitation of these vulnerabilities could allow an attacker to take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts. Failed exploitation attempts may result in a denial-of-service condition.

WINS Heap Overflow Vulnerability

This vulnerability may be triggered by sending a specially crafted WINS network packet to a either Windows 2000 Server or Windows Server 2003 running WINS.

WINS Integer Overflow Vulnerability
This vulnerability may be triggered by sending a specially crafted WINS network packet to a Windows 2000 Server running WINS. By default this vulnerability can only be successfully carried out from a trusted WINS replication partner. WINS replication partner is a host that is explicitly allowed to update another WINS server.

RECOMMENDATIONS:
The following actions should be taken:
Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
Ensure that all anti-virus software is up to date with the latest signatures.
Block un-trusted incoming traffic from the Internet at your network perimeter.

REFERENCES:

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1923
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1924

Microsoft:
http://www.microsoft.com/technet/security/bulletin/MS09-039.mspx

Security Focus
http://www.securityfocus.com/bid/35980
http://www.securityfocus.com/bid/35981

Secunia:
http://secunia.com/advisories/36213